Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

Relevant tcpdump Logs:

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150
```

The UDP protocol reveals that: DNS queries sent via UDP to the DNS server at 203.0.113.2 did not succeed, and instead triggered ICMP error responses.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unreachable.

The port noted in the error message is used for: Port 53, which is the standard port for DNS services.

The most likely issue is: The DNS server (203.0.113.2) was offline, misconfigured, or blocked by a firewall/router, causing DNS resolution failures.

Part 2: Explain your analysis of the data and provide at least one cause of the incident

Time incident occurred: Between 13:24:32 and 13:28:50, as shown in the tcpdump log timestamps.

Explain how the IT team became aware of the incident: Customers reported being unable to access the website www.yummyrecipesforme.com, and received the error 'destination port unreachable'.

Explain the actions taken by the IT department to investigate the incident: The IT team used tcpdump to analyze DNS traffic and found repeated ICMP messages indicating 'udp port 53 unreachable'.

Note key findings of the IT department's investigation: • DNS queries were correctly sent via UDP.
• ICMP responses confirmed port 53 was unreachable.
• No valid DNS responses were received, preventing domain resolution.

Note a likely cause of the incident: A DNS server outage, firewall misconfiguration, or network routing issue blocking UDP port 53 traffic.

Next steps for resolution: Verify that the DNS server is online and properly configured, check firewall rules to allow UDP port 53 traffic, and configure backup DNS servers for redundancy.